CLAIMS

1. A method for providing access to computer resources on a computer system, comprising:

generating a token containing encrypted user information including credit, authorization, and authentication information;

initiating a request to open a computer resource stored on the computer system, the computer resource being encrypted;

initiating execution of a remote application manager component on the computer system;

under control of the remote application manager component,

decrypting the token and authenticating a user of the computer system using authentication information stored in the token;

verifying whether the user is authorized to use the requested computer resource using authorization information stored in the token;

verifying whether the user has sufficient credit contained in the token to use the requested computer resource using credit information stored in the token;

when the user is authenticated, authorized, and has sufficient credit, decrypting and opening the requested computer resource;

monitoring the usage of the opened computer resource to determine whether the user has sufficient credit to continue using the computer resource; and

providing a notification when the monitored usage of the opened computer resource has exceeded the credit.

2. The method of claim 1 wherein generating a token comprises collecting authentication, authorization, and credit information from the user and storing the information in respective fields in a binary file, and thereafter encrypting the binary file to generate the token.

3. The method of claim 1 wherein the token is stored on a smart card that the remote application module component accesses to retrieve and decrypt the token.

4. The method of claim 1 wherein initiating a request to open a computer resource comprises clicking on an application icon.

5. The method of claim 1 wherein initiating execution of a remote application manager component occurs in response to initiating a request to open a computer resource.

6. The method of claim 1 wherein the token and the computer resource have been encrypted using the public key encryption methodology.

7. The method of claim 1 wherein the computer resource comprises an application module.

8. The method of claim 7 wherein the application module comprises an entire executable application program that is stored in encrypted form on the computer system.

9. The method of claim 1 wherein monitoring the usage of the opened computer resource comprises monitoring how long the user has been using the computer resource.

10. The method of claim 1 wherein providing a notification when the monitored usage of the opened computer resource has exceeded the credit comprises displaying a visual message to the user instructing the user to save his work and indicating his credit has been depleted.

11. A method for providing access to computer resources on a computer system, comprising:

under control of a client system,

providing user information to a server system, the user information including authentication, authorization, and credit information for a user of the client system;

receiving from the server system,

a token including encrypted information generated from the user information provided by the client system;

a remote application manager component;

at least one computer resource, each computer resource being encrypted and the particular computer resources received being determined from the authorization information contained in the provided user information;

under control of the remote application manager component on the client system,

decrypting the token in response to a request to initiate execution of one of the computer resources;

authenticating the user of the client computer system;

verifying whether the user is authorized to use the requested computer resource;

verifying whether the user has sufficient credit contained in the token to use the requested computer resource;

when the user is authenticated, authorized, and has sufficient credit, decrypting and initiating execution of the requested computer resource; and

monitoring the usage of the executing computer resource and providing a notification when the monitored usage has exceeded the user's credit.

12. The method of claim 11 wherein the token is stored on a smart card that the remote application module component accesses to retrieve and decrypt the token.

13. The method of claim 11 wherein a request to initiate execution of one of the computer resources comprises clicking on an application icon.

14. The method of claim 11 wherein the token and each computer resource have been encrypted using the public key encryption methodology.

15. The method of claim 11 wherein each computer resource comprises an application module.

16. The method of claim 15 wherein each application module comprises an entire executable application program that is stored in encrypted form on the computer system.

17. The method of claim 11 wherein monitoring the usage of the executing computer resource comprises monitoring how long the user has been using the computer resource.

18. The method of claim 11 wherein providing a notification when the monitored usage of the opened computer resource has exceeded the credit comprises displaying a visual message to the user instructing the user to save his work and indicating his credit has been depleted.

19. A method for providing access to computer resources on a computer system including client and server systems, comprising:

under control of a client system,

providing user information to a server system, the user information including authentication, authorization, and credit information for a user of the client system;

under control of a server system,

generating a token including encrypted information generated from the user information provided by the client system;

sending the token to the client system;

sending a remote application manager component to the client system;

sending at least one computer resource to the client system, each computer resource that is sent being encrypted;

under control of the remote application manager component on the client system,

initiating execution of the remote application manager component in response to a request to initiate execution of the computer resource;

decrypting the token and authenticating a user of the client computer system;

verifying whether the user is authorized to use the computer resource;

verifying whether the user has sufficient credit contained in the token to use the computer resource;

when the user is authenticated, authorized, and has sufficient credit, decrypting and initiating execution of the computer resource; and

monitoring the usage of the executing computer resource and providing notification when the monitored usage has exceeded the user's credit.

20. The method of claim 19 wherein the token is stored on a smart card that the remote application module component accesses to retrieve and decrypt the token.

21. The method of claim 19 wherein a request to initiate execution of one of the computer resources comprises clicking on an application icon.

22. The method of claim 19 wherein the token and each computer resource have been encrypted using the public key encryption methodology.

23. The method of claim 19 wherein each computer resource comprises an application module.

24. The method of claim 23 wherein each application module comprises an entire executable application program that is stored in encrypted form on the computer system.

25. The method of claim 19 wherein monitoring the usage of the executing computer resource comprises monitoring how long the user has been using the computer resource.

26. The method of claim 19 wherein providing a notification when the monitored usage of the opened computer resource has exceeded the credit comprises displaying a visual message to the user instructing the user to save his work and indicating his credit has been depleted.

27. A client system for providing access to computer resources, comprising:

a token component including encrypted user information, the user information including authentication, authorization, and credit information for a user of the client system;

at least one computer resource component, each computer resource component being encrypted;

a remote application manager component being adapted to receive the encrypted user information contained in the token, the remote application manager component operable responsive to a request to open a computer resource component to decrypt the encrypted user information, authenticate the user, determine whether the user is authorized to use the requested computer resource, and determine whether the user has sufficient credit to use the requested computer resource, the remote application manager component decrypting and opening the requested computer resource when the user is authenticated, authorized, and has sufficient credit,

and monitoring the usage of the opened computer resource and providing a notification when the monitored usage has exceeded the user's credit.

28. The client system of claim 27 wherein the request to initiate execution of a selected one of the computer resources comprises a request to initiate execution of a computer resource component not found on the client system, and the remote application manager component is further operable to contact a server system responsive to this request to initiate transfer of the selected computer resource component to the client system along with an updated token component including updated authorization information for the computer resource component.

29. The client system of claim 27 wherein the remote application manager is further operable to contact a server system when the credit contained in the token component is insufficient to initially open or to continue executing the selected computer resource component to initiate transfer of an updated token component including updated credit information to the client system.

30. The client system of claim 27 wherein the token component comprises a smart card on which the token is stored and a card reader that is adapted to read the token stored on the smart card and supply the read token to the remote application manager component.

31. A server system for providing access to computer resources, comprising:

a token generation component that is operable to receive user information including user authentication, authorization, and credit information, and operable to use the received user information in generating a token including encrypted user information;

a computer resource component including a plurality of computer resources; and

an accounting and billing component that is operable to receive user credit information and to verify user credit based upon such received information, the accounting and billing component providing a credit approval output indicating the results of the credit verification; and

a client interface component that is operable to receive client requests from client computers and to provide credit information contained in such requests to the accounting and billing component, and when the credit approval output indicates the user's credit has been approved the client interface component providing credit and user information to the token generation component and receiving the generated token from the token generation component, the client interface component further operable to select computer resources using information contained in the client requests and to encrypt each selected computer resource, the client interface module transferring the token and the encrypted selected computer resources to the client computer along with a remote application manager component.

32. The server system of claim 31 wherein the computer resource component includes a plurality of application programs.

33. The server system of claim 32 wherein each of the application programs includes all necessary system files for execution.

34. The server system of claim 31 wherein the client interface component is adapted to receive HTTP requests from client computers and each client request is received as one or more such HTTP requests.